NEWMEYER & DILLION LLP

What to Do When the Worst Happens: Responding to A Cybersecurity Breach

By: Scott L. Satkin & J. Kyle Janecek

Scott L. Satkin

Contact

949.271.7204
scott.satkin@ndlf.com

Practice Areas

Business Litigation
Business Transactions
Privacy & Data Security
Insurance Law
Real Estate Litigation
Real Estate Transactions

J. Kyle Janecek

Contact

949.854.7099
kyle.janecek@ndlf.com

Practice Areas

Business Transactions
Corporate Matters
Lending & Finance
Privacy & Data Security
Real Estate Transactions

Cybersecurity is a growing concern for today's businesses. While it's always advisable to take whatever action possible to avoid a cybersecurity breach, no security measures can be one hundred percent perfect, and malicious actors are always innovating and trying to find new security flaws. The implementation of new technology brings with it new opportunities, but also potentially new vulnerabilities. And hackers have one major advantage – those working to defend against cyber-attacks have to try to find and fix every potential exploit, whereas those on the other side only need to find one. As demonstrated by recent high-profile breaches at Google and Facebook, even massive tech companies with access to vast financial resources and top engineering talent can still fall prey to cyber-attacks. Therefore, understanding how to respond to a breach is just as critical to a company's cybersecurity plan as attempting to prevent one. Below are a few solid tips on how to react when an organization's cybersecurity has been compromised.

Plan in Advance

The best response to a cybersecurity breach begins before the breach ever happens. A written incident response plan is of paramount importance. In the immediate aftermath of a cybersecurity breach, people will be scared and stressed. In those circumstances, they will be more likely to be able to respond effectively if there is a plan laid out for them and they have received training on how to follow that plan. Make sure that employees are trained on the parts of the plan that are relevant to them. Most may only need to know who to report to if they suspect a breach may have occurred, while those who will be involved in the breach response will need more in-depth training. The plan should also be updated regularly to account for staffing changes, new technology, and the evolving legal landscape. The law may also require a plan for responding to cybersecurity breaches, depending on the jurisdiction.

Call Your Lawyer- Early and Often

At the risk of sounding self-aggrandizing, attorneys are critical in responding to a cybersecurity breach. The most obvious reason is to advise clients on their legal obligations and potential liability – and this is indeed an important function. The patchwork of federal and state regulations governing cybersecurity is something laypeople – and even non-specialized attorneys – should navigate with caution. Of equal importance is the preservation of confidential communication under the attorney-client privilege. The presence of an attorney helps to improve the security of information surrounding the response to the breach because correspondence with that attorney

is privileged, allowing candid evaluation of the breach. The ability to assert attorney-client privilege regarding an internal investigation and response can be quite useful in the event of a later external investigation or litigation.

To Diclose or Not to Disclose?

An important question that needs to be asked in the wake of a cybersecurity breach is whether the incident must be disclosed, and if so, when, how, and to whom should such disclosures be made? While many understandably wish that their mistakes and failures will never see the light of day, there are also many people who will want to know when a company's cybersecurity has been breached. Shareholders want to know – and may have a right to know – if such a breach has harmed the business. Consumers want to know if their personal information has been compromised so that they can protect against identity theft. Furthermore, state breach notification laws may mandate certain disclosures to consumers depending on facts surrounding the breach. Legal requirements from states, the federal government, and even foreign entities may also require companies to provide notices to one or more regulatory agencies.

An attorney can advise on whether a company is legally required to provide any notice in the aftermath of a data breach, but even though notice may not be a legal requirement in a particular set of circumstances, it may still be prudent to give it anyway. Google decided not to disclose the recent breach of data from its Google+ service to avoid a PR and regulatory backlash, but the fact that it had happened eventually leaked out anyway. Even though legal experts have opined in the aftermath that Google likely was not obligated to disclose the breach, the fact that it did not caused exactly what Google attempted to avoid, but with magnified effect. "Google Experiences Consumer Data Breach" may not have been a good headline, but "Google Hides Consumer Data Breach" was a worse one.

Remember: Protection is Key

No company wants a cybersecurity breach, but past experience has increasingly demonstrated that this is not a question of "if" but rather one of "when" and "how bad." Planning ahead and knowing what to do when a data breach does happen can ensure that an organization bounces back from a breach as smoothly and painlessly as possible.

Scott Satkin and Kyle Janecek are associates in the Cybersecurity group of Newmeyer & Dillion. Focused on helping clients navigate the legal dispute implications of cybersecurity, they advise businesses on implementing and adopting proactive measures to prevent and neutralize cybersecurity threats. For questions on how they can help, contact Scott at scott.satkin@ndlf.com and Kyle at kyle.janecek@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of cybersecurity, business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America© and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.